EAST Search History

<table>
<tr><th>Ref #</th><th>Hits</th><th>Search Query</th><th>DBs</th><th>Default Operator</th><th>Plurals</th><th>Time Stamp</th></tr>
<tr><td>S1</td><td>4</td><td>("20010034841"|"5535279"|"6088451"|"6148404").PN.</td><td>US-PGPUB; USPAT</td><td>OR</td><td>ON</td><td>2007/08/29 13:06</td></tr>
<tr><td>S2</td><td>9</td><td>("20020112155"|"20020133723"|"20020150253"|"20020152393"|"20030149880"|"20030163691"|"5944824"|"6246771"|"6725376").PN.</td><td>US-PGPUB; USPAT</td><td>OR</td><td>ON</td><td>2007/08/24 12:33</td></tr>
<tr><td>S3</td><td>6</td><td>("20010037462"|"20030093694"|"20050074126"|"5812776"|"5987232"|"6363365").PN.</td><td>US-PGPUB; USPAT</td><td>OR</td><td>ON</td><td>2007/08/24 12:34</td></tr>
<tr><td>S4</td><td>3</td><td>("20020095389"|"20050074126"|"6981156").PN.</td><td>US-PGPUB; USPAT</td><td>OR</td><td>ON</td><td>2007/08/24 12:35</td></tr>
<tr><td>S5</td><td>2</td><td>recovering adj password adj protected adj private</td><td>US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB</td><td>OR</td><td>ON</td><td>2007/08/29 13:32</td></tr>
<tr><td>S6</td><td>4</td><td>("20010034841"|"5535279"|"6088451"|"6148404").PN.</td><td>US-PGPUB; USPAT</td><td>OR</td><td>ON</td><td>2007/08/29 13:32</td></tr>
<tr><td>S7</td><td>9</td><td>("20020112155"|"20020133723"|"20020150253"|"20020152393"|"20030149880"|"20030163691"|"5944824"|"6246771"|"6725376").PN.</td><td>US-PGPUB; USPAT</td><td>OR</td><td>ON</td><td>2007/08/29 13:32</td></tr>
<tr><td>S8</td><td>6</td><td>("20010037462"|"20030093694"|"20050074126"|"5812776"|"5987232"|"6363365").PN.</td><td>US-PGPUB; USPAT</td><td>OR</td><td>ON</td><td>2007/08/29 13:32</td></tr>
<tr><td>S9</td><td>3</td><td>("20020095389"|"20050074126"|"6981156").PN.</td><td>US-PGPUB; USPAT</td><td>OR</td><td>ON</td><td>2007/08/29 13:32</td></tr>
<tr><td>S10</td><td>21</td><td>S6 or S7 or S8 or S9</td><td>US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB</td><td>OR</td><td>ON</td><td>2007/08/29 14:05</td></tr>
<tr><td>S11</td><td>103</td><td>380/286.ccls. and (password passcode)</td><td>US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB</td><td>OR</td><td>ON</td><td>2007/08/29 14:05</td></tr>
<tr><td>S12</td><td>53</td><td>("5436972").URPN.</td><td>USPAT</td><td>OR</td><td>ON</td><td>2007/08/30 13:17</td></tr>
<tr><td>S13</td><td>39</td><td>("6044155").URPN.</td><td>USPAT</td><td>OR</td><td>ON</td><td>2007/08/29 19:47</td></tr>
<tr><td>S14</td><td>53</td><td>("5436972").URPN.</td><td>USPAT</td><td>OR</td><td>ON</td><td>2007/08/30 13:18</td></tr>
<tr><td>S15</td><td>39</td><td>("6044155").URPN.</td><td>USPAT</td><td>OR</td><td>ON</td><td>2007/08/30 13:18</td></tr>
</table>

EAST Search History

S16	92	S14 or S15	US-PGPUB; USPAT	OR	ON	2007/08/30 13:18
S17	30	(user adj key) same repository	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/08/30 22:22
S18	14	("5237610" | "5481613" | "5757913"). PN. OR ("6160891").URPN.	US-PGPUB; USPAT; USOCR	OR	ON	2007/08/30 15:40
S19	91	(key adj recovery) same server	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/08/30 22:22
S20	91	(key adj recovery) same server	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/08/31 11:19
S21	1	"20050223216".pn.	US-PGPUB	OR	ON	2007/09/02 18:49
S22	14	(US-20010034841-$ or US-20050223216-$ or US-20040228493-$ or US-20020071567-$).did. or (US-6246771-$ or US-5937066-$ or US-6931133-$ or US-6754349-$ or US-6266421-$ or US-6044155-$ or US-6160891-$ or US-7203844-$ or US-6118874-$ or US-6760752-$).did.	US-PGPUB; USPAT	OR	ON	2007/09/02 22:22
S23	3	S22 and (forget forgot)	US-PGPUB; USPAT	OR	ON	2007/09/02 22:58
S24	6	S22 and (lose)	US-PGPUB; USPAT	OR	ON	2007/09/02 23:08
S25	11	380/286.ccls. and (backup adj key)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/09/02 23:08

PORTAL
USPTO

Subscribe (Full Service) Register (Limited Service, Free) Login

Search: ● The ACM Digital Library ○ The Guide

+backup +"key escrow" SEARCH

THE ACM DIGITAL LIBRARY

Feedback Report a problem Satisfaction survey

Published before May 2004
Terms used: **backup key escrow**

Found **14** of **154,987**

Sort results by relevance ▾
Display results expanded form ▾

Save results to a Binder
? Search Tips
□ Open results in a new window

Try an Advanced Search
Try this search in The ACM Guide

Results 1 - 14 of 14

Relevance scale □ ▂ ▄ ▆ ■

1 Crypto backup and key escrow ■
David Paul Maher
March 1996 **Communications of the ACM**, Volume 39 Issue 3
Publisher: ACM Press
Full text available: pdf(498.27 KB) Additional Information: full citation, references, citings, index terms

2 A taxonomy for key escrow encryption systems ■
Dorothy E. Denning, Dennis K. Branstad
March 1996 **Communications of the ACM**, Volume 39 Issue 3
Publisher: ACM Press
Full text available: pdf(548.67 KB) Additional Information: full citation, citings, index terms, review

3 The Ω key management service ■
Michael K. Reiter, Matthew K. Franklin, John B. Lacy, Rebecca N. Wright
January 1996 **Proceedings of the 3rd ACM conference on Computer and communications security CCS '96**
Publisher: ACM Press
Full text available: pdf(1.37 MB) Additional Information: full citation, references, citings, index terms

4 Securing wireless applications: ESCORT: a decentralized and localized access control system for mobile wireless access to secured domains ■
Jiejun Kong, Shirshanka Das, Edward Tsai, Mario Gerla
September 2003 **Proceedings of the 2003 ACM workshop on Wireless security WiSe '03**
Publisher: ACM Press
Full text available: pdf(401.72 KB) Additional Information: full citation, abstract, references, citings, index terms

In this work we design and implement ESCORT, a *backward compatible*, *efficient*, and *secure* access control system, to facilitate mobile wireless access to secured wireless LANs. In mobile environments, a mobile guest may frequently roam into foreign domains while demanding critical network services. ESCORT provides instant yet secure access to the mobile guest based on the concept of "*escort*", which refers to a special network object with four distinct properties: (1) T ...

Keywords: decentralized access control, identity privacy, location privacy, mobile privacy, wireless security

5 Identification control: Owner-controlled information
Carrie Gates, Jacob Slonim
August 2003 **Proceedings of the 2003 workshop on New security paradigms NSPW '03**
Publisher: ACM Press
Full text available: pdf(1.06 MB) Additional Information: full citation, abstract, references

Information about individuals is currently maintained in many thousands of databases, with much of that information, such as name and address, replicated across multiple databases. However, this proliferation of personal information raises issues of privacy for the individual, as well as maintenance issues in terms of the accuracy of the information. Ideally, each individual would own, maintain and control his personal information, allowing access to those who needed at the time it was needed. O ...

Keywords: architecture, privacy, security

6 How to break fraud-detectable key recovery
Birgit Pfitzmann, Michael Waidner
January 1998 **ACM SIGOPS Operating Systems Review**, Volume 32 Issue 1
Publisher: ACM Press
Full text available: pdf(417.38 KB) Additional Information: full citation, abstract, index terms

Fraud detection for software key recovery schemes means that, without knowing the session key, a third party can verify whether the correct session key could be recovered. This concept and a construction by so-called binding data was introduced by Verheul et al. at Eurocrypt '97 to provide for dishonest users that make simple modifications to messages, e.g., delete the key recovery information, and manipulate the recipient's software such that it decrypts messages even if the key recovery inform ...

7 An authorization model for a public key management service
Pierangela Samarati, Michael K. Reiter, Sushil Jajodia
November 2001 **ACM Transactions on Information and System Security (TISSEC)**, Volume 4 Issue 4
Publisher: ACM Press
Full text available: pdf(337.73 KB) Additional Information: full citation, abstract, references, citings, index terms, review

Public key management has received considerable attention from both the research and commercial communities as a useful primitive for secure electronic commerce and secure communication. While the mechanics of certifying and revoking public keys and escrowing and recovering private keys have been widely explored, less attention has been paid to access control frameworks for regulating access to stored keys by different parties. In this article we propose such a framework for a key management ser ...

Keywords: Access control, authorizations specification and enforcement, public key infrastructure

8 Inside Risks: Digital evidence
David WJ Stringer-Calvert
April 2002 **Communications of the ACM**, Volume 45 Issue 4
Publisher: ACM Press
Full text available: pdf(95.78 KB) html(7.81 KB) Additional Information: full citation, index terms

9 Unlinkable serial transactions: protocols and applications
Stuart G. Stubblebine, Paul F. Syverson, David M. Goldschlag
November 1999 **ACM Transactions on Information and System Security (TISSEC)**, Volume 2 Issue 4
Publisher: ACM Press
Full text available: pdf(184.87 KB) Additional Information: full citation, abstract, references, citings, index terms, review

We present a protocol for unlinkable serial transactions suitable for a variety of network-based subscription services. It is the first protocol to use cryptographic blinding to enable subscription services. The protocol prevents the service from tracking the behavior of its customers, while protecting the service vendor from abuse due to simultaneous or cloned use by a single subscriber. Our basic protocol structure and recovery protocol are robust against failure in protocol termination. ...

Keywords: anoymity, blinding, cryptographic protocols, unlinkable serial transactions

10 The network society as seen by two European underdogs
Andrea Monti
April 2000 **Proceedings of the tenth conference on Computers, freedom and privacy: challenging the assumptions CFP '00**
Publisher: ACM Press
Full text available: pdf(61.06 KB) Additional Information: full citation, index terms

11 Risks to the public in computers and related systems
Peter G. Neumann
May 1998 **ACM SIGSOFT Software Engineering Notes**, Volume 23 Issue 3
Publisher: ACM Press
Full text available: pdf(789.30 KB) Additional Information: full citation, index terms

12 The economics of information security investment
Lawrence A. Gordon, Martin P. Loeb
November 2002 **ACM Transactions on Information and System Security (TISSEC)**, Volume 5 Issue 4
Publisher: ACM Press
Full text available: pdf(461.31 KB) Additional Information: full citation, abstract, references, citings, index terms, review

This article presents an economic model that determines the optimal amount to invest to protect a given set of information. The model takes into account the vulnerability of the information to a security breach and the potential loss should such a breach occur. It is shown that for a given potential loss, a firm should not necessarily focus its investments on information sets with the highest vulnerability. Since extremely vulnerable information sets may be inordinately expensive to protect, a f ...

Keywords: Optimal security investment

13 COCA: A secure distributed online certification authority
Lidong Zhou, Fred B. Schneider, Robbert Van Renesse
November 2002 **ACM Transactions on Computer Systems (TOCS)**, Volume 20 Issue 4
Publisher: ACM Press
Full text available: pdf(448.28 KB) Additional Information: full citation, abstract, references, citings, index terms

COCA is a fault-tolerant and secure online certification authority that has been built and deployed both in a local area network and in the Internet. Extremely weak assumptions characterize environments in which COCA's protocols execute correctly: no assumption is made about execution speed and message delivery delays; channels are expected to exhibit only intermittent reliability; and with $3t + 1$ COCA servers up to t may be faulty or compromised. COCA is the first system to integr ...

Keywords: Byzantine quorum systems, Certification authority, denial of service, proactive secret-sharing, public key infrastructure, threshold cryptography

14 Risks to the public in computers and related systems
Peter G. Neumann
January 1997 **ACM SIGSOFT Software Engineering Notes**, Volume 22 Issue 1
Publisher: ACM Press
Full text available: pdf(809.47 KB) Additional Information: full citation, index terms

Results 1 - 14 of 14